Amendments to the Specification

Please replace the paragraph at page 1, lines 19 to 23 with the following amended paragraph:

a1

Digital signatures with message recovery are categorized by the fact that the message is not required as input to the verification algorithm. ~~One problem with~~ One goal when designing message recovery schemes is to defeat existential forgery attacks by defining a suitable redundancy function which will distinguish messages legitimately signed from signatures of random bit strings.